REMARKS

The Office Action of July 19, 2006 has been carefully reviewed and these remarks are responsive thereto. Claims 1, 2, 19, 21, 24, 26, 27, and 45 have been amended, no claims have been cancelled, and claims 59 and 60 have been added. Claims 1-2, 4-13, 15, 19-22, 24, 26-32, 34-38, and 45-60 remain pending in this application. Reconsideration and allowance of the instant application are respectfully requested.

Rejections Under 35 U.S.C. § 112

Claims 57 and 58 stand rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement. Applicants respectfully traverse.

Claim 57 recites a "method of communicating between a first computer protected by a first firewall and a second computer protected by a different second firewall." Support for this recitation can be found, e.g., in FIGS. 1-3, and at paragraph [0008] of the specification as originally filed. Claim 57 further recites:

> (1) at a third computer situated between the first firewall and the different second firewall, receiving a first HTTP message from the first computer through a port in the first firewall that is configured to be open to outgoing HTTP traffic and open to incoming HTTP traffic that is responsive to and linked to outgoing HTTP traffic; **[support for which can be found at, e.g., FIGS. 1-3, and at paragraph [0008] of the specification as originally filed]**

> (2) from the third computer, sending a first response message to the first computer through the port in the first firewall, thereby establishing a first receive channel through the first firewall, wherein the first response message is linked to the first HTTP message; **[support for which can be found at, e.g., FIGS. 1-3, and at paragraph [0061] of the specification as originally filed]**

> (3) at the third computer, receiving a second HTTP message from the second computer through a port in the different second firewall that is configured to be open to outgoing HTTP traffic and open to incoming HTTP traffic that is responsive to and linked to outgoing HTTP traffic; **[support for which can be found at, e.g., FIGS. 1-3, and at paragraph [0008] and [0040] of the specification as originally filed]**

> (4) from the third computer, sending a second response message to the second computer through the port in the different second firewall, thereby establishing a second receive channel through the second firewall, wherein

14

the second response message is linked to the second HTTP message; **[support for which can be found at, e.g., FIGS. 5A-5C, and at paragraphs [0036], [0061], and [0143] of the specification as originally filed]**

(5) at the third computer, receiving a third encrypted HTTP message from the first computer through the port in the first firewall; determining that the third encrypted HTTP message is intended to be delivered to the second computer, and transmitting to the second computer the third encrypted HTTP message, wherein the third encrypted HTTP message is transmitted over the second receive channel to the second computer; and **[support for which can be found at, e.g., FIGS. 1-3 and 5A-5C, and at paragraphs [0008] and [0077] of the specification as originally filed]**

(6) from the third computer, periodically transmitting "keep alive" messages to the first and second computers to avoid a time-out condition. **[support for which can be found at, e.g., FIGS. 1-3, and at paragraph [0107] of the specification as originally filed]**

Claim 58 recites, "wherein step (5) is performed at the third computer by transmitting the third encrypted HTTP message to the second computer without decrypting contents of the third encrypted HTTP message." Support for this recitation can also be found, e.g., in FIGS. 1-3, and at paragraphs [0008] and [0040] of the specification as originally filed.

Claims 5 and 35 stand rejected under 35 U.S.C. § 112, second paragraph, as being indefinite. Specifically, the office action states, "[i]n the present instance, claim 5 recites the broad recitation wherein said open port is at least one of port 80 and port 8080, and the claim 1 recites port that is normally open to HTTP packets which is the narrower statement of the range/limitation." Applicants respectfully traverse. Claim 5 specifies port numbers through which the HTTP message is transmitted. The range of port numbers recited in claim 5 is not open-ended, and therefore narrows the transmitting feature of claim 1, which does not recite any port numbers. MPEP § 2173(c). Accordingly, Applicants respectfully request the rejection be withdrawn.

Rejections Under 35 U.S.C. § 103

Claims 1, 2, 4-13, 15, 19-22, 24, 26-32, 34-38, and 45-58 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,101,543 (Alden), in view of TunnelBuilder 4.01 for Windows Website (WinTB). Applicants respectfully traverse this rejection for at least the following reasons.

Claims 55-58

Preliminarily, Applicants note that the office action fails to address or provide reasonable grounds for rejection for many of the features recited in claims 16-58. The office action states on page 9 that these claims "disclose the same invention with similar claim limitations therefore the rejection applied to claims 1-15 applies equally to as well to claims 16-58." Applicants disagree with this characterization, especially with regard to claims 55-58, and respectfully request that the office discuss all of the features of the recited claims with reference to prior art teachings so that Applicants may have a reasonable opportunity to respond.

For example, claim 55 recites, "receiving from the intermediate server computer a response including a connection identifier corresponding to the first return path," and "creating a second return path between the second computer and the intermediate server computer." None of the claims 1-15 recite creating a return path between the intermediate server and either the transmitting or receiving computer, and neither Alden nor WinTB teaches or suggests an intermediate server that transmits or receives a "connection identifier corresponding to the first return path" as recited in claim 55.

Claim 55 further recites, "periodically transmitting from the intermediate server computer to the first computer a 'keep alive' message if no further messages are received from the first computer within a period of time." Claim 57 includes a similar recitation. Neither the cited portions of Alden and WinTB, nor any other portion of these references that Applicants have identified, teaches or suggests "keep alive" messages. Thus, independent claims 55 and 57 are allowable over the cited references. Dependent claims 56 and 58-60 are allowable for at least the same reasons as their respective base claims, as well as based on additional features recited therein.

For example, claim 56 recites, "in the intermediate server computer, decrypting encrypted information received from the first computer using encryption keys shared between the first computer and the intermediate computer, and then re-encrypting the received information using encryption keys shared between the intermediate computer and the second computer." Alden discloses a pseudo network adapter for establishing tunnel connections between endpoints separated by firewalls. (Alden, Abstract; FIG. 3, col. 6, line 46 to col. 7, line 17.) However, the only encryption disclosed by Alden and similar tunneling systems takes place between the two

endpoints of the tunnel connection. (Alden, col. 8, lines 31-56.) Accordingly, neither Alden nor WinTB teaches an intermediate server "decrypting encrypted information," as recited. Claim 56 is allowable for this additional reason.

As mentioned above, the office action fails to identify the teaching or suggestion in the cited references for "receiving from the intermediate server a ... connection identifier corresponding to a return path," as recited in claim 55, a "keep alive" message as recited in claims 55 and 57, or an intermediate server "decrypting encrypted information," as recited in claim 56.

Accordingly, Applicants respectfully request that a subsequent office action that substantively addresses claims 55-58 should also be non-final to provide Applicants an opportunity to respond to such rejections when first presented.

Claims 47-60

Claim 47 recites a method of transferring data that may be performed by a computer, for example, a server similar to the intermediate servers discussed above in reference to claims 55-58. Specifically, claim 47 recites receiving a first HTTP message from a first computer through a first firewall and receiving a second HTTP message from a second computer through a second firewall, "wherein the second message causes a return path to be established to the second computer." In neither Alden nor WinTB, is a message corresponding to this "second message" ever transmitted. In Alden, a message is sent from a first tunnel server to a second tunnel server via one or more tunnel relays and firewalls connecting the two servers. (Alden, FIG. 3; col. 6, line 46 to col. 7, line 17.) However, Alden's second tunnel server will only be able to receive the message if its firewall is "programmed to pass packets received over transport layer connection 2 into a private network on the other of the firewall." (Alden, col. 6, lines 37-39.) The reason for this is that Alden's technique does not involve establishing a return path to the recipient computer, as recited in claim 47. The "second HTTP message [that] causes a return path to be established to the second computer," as recited in claim 47, allows the second computer a transmission channel through which it may receive messages from the first computer, without the need for modifying or programming the firewall associated with the second computer. Since neither Alden nor WinTB teaches or suggests "a second message [that] causes a return path to be established to the second computer," Applicants submit that claim 47 is not obvious over the

17

cited references. Claims 48-54 depend from claim 47, and are allowable for at least the same reasons, as well as based on the additional features recited therein.

Claims 55-60 are similarly distinguishable.

Even if Alden used port 80, it will not function without a firewall modification. The reason is that normal port 80 firewall connections are only enabled from behind the firewall out to the public Internet. Connections cannot be initiated from the public Internet to a computer behind the firewall on a private network. The firewall blocks these connections. As shown in FIG. 4 of Alden, a connection is made from node C to node D. This connection could not be made without a firewall modification, even if port 80 is used.

WinTB uses the exact same technique as Alden in this respect, and would not work without firewall modifications for the same reason.

Although HTTP is referred to in WinTB, apparently because it uses outbound port 80 for the initiating side of the connection, usually labeled node A, WinTB requires a firewall modification on the non-initiating node (e.g., node D in FIG. 4 of Alden). The non-initiating node is usually a server located on a corporate network so that firewall modification is considered easy. Both systems will not function over normal firewalls port 80 settings. In fact there is more to it. Port 80 must be opened and the routing must be defined to send port 80 traffic to that specific computer.

Claims 1-46

Claim 1, as amended, recites transmission of an HTTP message "comprising an encrypted identifier of said second computer and encrypted content, wherein the identifier is encrypted with a first encryption key associated with the server and the content is encrypted with a second different encryption key associated with the second computer." As mentioned above, Alden discloses a pseudo network adapter for establishing tunnel connections between endpoints separated by firewalls. (Alden, Abstract; FIG. 3, col. 6, line 46 to col. 7, line 17.) However, the only encryption disclosed by Alden and similar tunneling systems takes place between the two endpoints of the tunnel connection. (Alden, col. 8, lines 31-56.) Through the key exchange / authentication request and response frames, Alden's tunnel endpoints (node A and node D in FIG. 3) may be configured to encrypt / decrypt data. However, Alden's tunnel relays (node B and node C in FIG. 3) do not exchange encryption keys with the tunnel endpoints, and are thus

18

not capable of encrypting / decrypting any data. Instead, there relays merely forward the data frames between the two endpoints. Thus, neither Alden's tunnel endpoints nor tunnel relays could perform the functions of the server in claim 1, which "decrypts said encrypted identifier to an unencrypted identification of said second computer and forwards said encrypted content to said second computer using said unencrypted identification." For similar reasons, Alden does not teach or suggest transmitting an HTTP message "comprising an encrypted identifier of said second computer and encrypted content, wherein the identifier is encrypted with a first encryption key associated with the server and the content is encrypted with a second different encryption key associated with the second computer."

WinTB also does not disclose or suggest a server which "decrypts said encrypted identifier to an unencrypted identification of said second computer and forwards said encrypted content to said second computer using said unencrypted identification," or transmitting an HTTP message "comprising an encrypted identifier of said second computer and encrypted content, wherein the identifier is encrypted with a first encryption key associated with the server and the content is encrypted with a second different encryption key associated with the second computer," as recited in claim 1. Thus, claim 1 is allowable over the cited references. Claims 2, 4-13, and 15 depend from independent claim 1 and are allowable for at least the same reasons as claim 1, as well as based on additional features recited therein.

Independent claims 19, 21, 24, 26, 27, and 45 each contain at least one similar limitation as referred to above with respect to claim 1, and are thus allowable for at least the same reasons as claim 1. Dependent claims 20, 22, 28-32, 34-38, and 46 are allowable for at least the same reasons as their respective base claims, and further based on the additional features recited therein.

New Claims

Applicants have added new claims 59 and 60 to more fully claim their invention. Dependent claim 59 recites a message comprising, "an identifier of said second computer encrypted with a first encryption key associated with the intermediate server, and ... information ... encrypted with a second different encryption key associated with the second computer." Dependent claim 60 contains a similar recitation. As described above with respect to claim 1, Alden and WinTB fail to teach or suggest encrypting a computer identifier with a first encryption

19

key and encrypting message content with a second different encryption key. Applicants therefore submit that new claims 59 and 60 are allowable over the cited references.
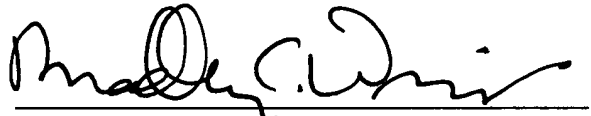
Conclusion

Based on the foregoing, Applicants respectfully submit that the application is in condition for allowance and a Notice to that effect is earnestly solicited. Should the Examiner believe that anything further is desirable in order to place the application in even better form for allowance, the Examiner is respectfully urged to contact Applicants' undersigned representative at the below-listed number.

Respectfully submitted,

BANNER & WITCOFF, LTD.

Dated this 19 day of Oct. , 2006   By: _____

Bradley C. Wright
Registration No. 38,061

1001 G Street, N.W.
Washington, D.C. 20001-4597
Tel: (202) 824-3160
Fax: (202) 824-3001